VPN에서의 이상행동 탐지를 활용한 정보유출 방지에 관한 연구+

박장수, 김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[pjswise, kimsh, imylee]@sch.ac.kr

A study on Preventing Data Leakage using Abnormal Behavior Detection in a Virtual Private Network

Jang-Su Park, Su-Hyun Kim, Im-Yeong Lee
Dept of Computer Software Engineering, SoonChunHyang University

요 약

최근 IT기술과 인터넷의 발전으로 시간과 공간에 제한을 두지 않고 업무를 처리해야 하는 상황으로 업무환경이 급격히 변화되고 있다. 특히 기업에서는 외부 네트워크와 정보교환의 필요성이 증가되었고, 구성원들의 잦은 외근, 출장 등 사무실 밖에서 업무를 처리하는 비중이 높아져, 내부뿐만 아니라 외부와의 정보공유를 하는데 있어 안전한 네트워크 구조를 요구하고 있다. 외부에서 효율적이고 안전하게 내부시스템에 접속할 수 있게 사용되는 것이 VPN(가상사설망: Virtual Private Network)으로, 기관 및 기업에서 VPN을 지속적으로 도입하여 운영하고 있다. 하지만 VPN에 인증이 성공되면 다양한 업무 시스템에 접근이 용이하기 때문에, 악의적인 사용자로부터 정보유출이 손쉽게 이루어질 수 있다. 따라서 본 연구에서는 사용되고 있는 VPN에 대해 관리가 잘 이루어지는지 확인하는 실태점검 리스트를 제시하고, VPN에 대한 정보유출방지 모니터링을 위해 VPN의 접속로그를 분석하여 정보유출 보안위협 행위를 탐지할 수 있는 시나리오를 도출하고자 한다.

1. 서론

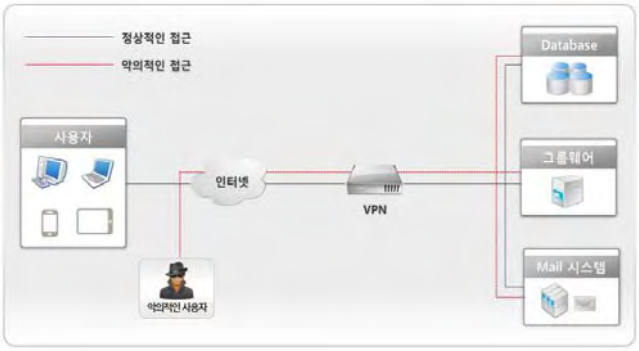
최근 네트워크의 발달과 모바일 단말기의 확산으로 사무실에서만 근무를 하지 않고 외근, 출장 등 사무실 밖에서 업무를 처리하는 비중이 높아지고 있으며, 재택근무가 부분적으로 확대되고 있다. 또한 시간과 장소에 제한 없이 업무를 수행할 수 있는 새로운 근무 환경인 스마트워크 개념이 도입되고 있다. 이러한 새로운 환경은 유연한 근무 환경을 조성하지만, 중요정보(개인정보, 핵심기술정보 등)의 유출 가능성이 있다는 보안위협이 존재한다. 따라서 다양한 기관 및 기업에서는 원격지에서 인터넷을 이용해 내부 정보시스템을 안전하게 사용할 수 있도록 지원하는 기술로 VPN을 도입하여 운영하고 있다. 하지만 VPN을 사용하는 경우 송수신 데이터에 대한 암호화를 통해 안전한 통신수단을 제공하고 있지만, 대부분의 VPN의 장비들은 아이디/패스워드 기반의 사용자 인증만으로 인증을 수행하고 있다. 이는 정상적인 사용자의 계정을 탈취하거나 도용된다면 내부 업무시스템에 접근이 용이하고, 이를 탐지하기에는 매우 어려움이 존재한다. 따라서 본 논문에서는 VPN에서 발생하는 접속 로그들을 분석하여 사용자의 이상행위를 도출하고, 이를 기반으로 정보유출방지를 위한 모니터링 방법론을 제시하고자한다.

+ 본 논문은 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0221609)의 연구수행으로 인한 결과물임을 밝힙니다.

2. VPN을 통한 정보유출 경로 및 문제점

인터넷과 같은 공중망을 이용하여 사설망의 효과를 얻을수 있는 기술로 이를 구현하기 위한 하드웨어 및 소프트웨어를 VPN이라고 한다. SSL VPN기술을 이용하면 표준 웹 브라우저를 이용하여 간편한 사내 접속이 가능하다. VPN은 접속 방식에 따라 인트라넷 VPN, 익스트라넷 VPN, 원격접속 VPN으로 분류된다.

이러한 VPN 장비들은 아이디/패스워드 기반의 사용자 인증을 통해 기관 및 기업의 인트라넷에 접속할 수 있게 되고, 다양한 업무시스템에 접근할 수 있기 때문에 정보유출 사고가 발생할 수 있는 위협이 존재한다. 이를 해결하기 위해 현재 VPN에서는 2Factor 인증을 적용함으로써, VPN 접근에 대한 강화를 하고 있다. 하지만 사용자 인증만을 강력하게 하였다고 하여 보안 사고를 예방할 수는 없다. (그림 1)에서와 같이 악의적인 내부자에 의해 정상적인 사용자의 계정을 탈취하거나 도용을 하여 내부 업무시스템에 접근을 한다면, 이상행동에 대한 탐지가 어렵다. 따라서 정보유출 방지를 위해서는 VPN에 대한 접근로그에서 이상행동을 살펴볼 필요가 있다.



(그림 1) VPN을 통한 정보유출 경로

3. VPN에서의 정보유출방지 모니터링 방안

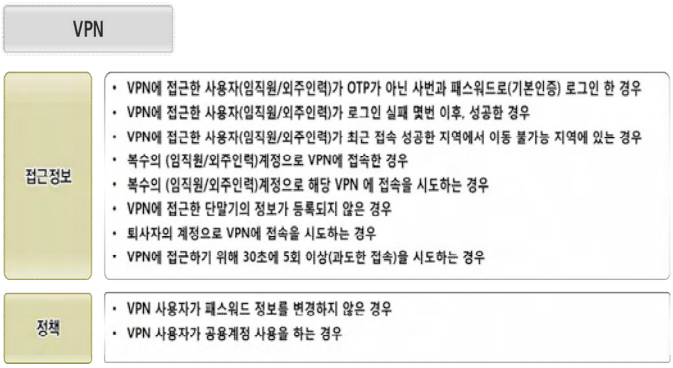
본 장에서는 기 운영중인 VPN이 안전성을 위한 보안 관리가 지속적으로 되고 있는지 각 기업 및 기관의 보안 담당자가 체크할 수 있는 실태점검 리스트를 제시한다. 또한 VPN 접속로그 중에서 이상행동을 탐지할 수 있는 정보유출 시나리오를 도출하여, 모니터링방안에 대한 프로세스를 설명한다.

3.1 VPN 실태점검 리스트

정보유출사고를 위한 대응방안으로는 사전적으로 정보유출가능성을 예상하고 해당 보안솔루션을 도입하여 운영하는 방안과 사후적으로 정보유출이 발생하였을 경우 이로 인한 피해발생을 최소화 하는 대응체계를 마련하는 것이 있을 수 있다. 마지막으로 현재 기 구축되어 운영하고 있는 보안솔루션에 대해 지속적인 개선 및 관리가 이루어지는지 실태점검 확인이 필요하다. 보안솔루션을 도입하여 운영중이더라도 지속적인 관리를 하지 않으면 또 다른 보안 사고를 야기시킬 수 있기 때문이다. 하지만 각 보안솔루션에 대한 이해와 운영 부족 및 가이드라인 미비 등의 이유로 기업 및 기관의 보안담당자들은 각 장비의 실태점검을 수행하지 않는 경우가 대부분이다. 기관 및 기업에서 기 사용중인 VPN에 대해 관리가 지속적으로 되고 있는지 보안담당자가 체크할 수 있는 실태점검 리스트를 통해 현 상황을 알아볼 필요성이 있다. 따라서 본 연구에서는 8개 항목으로 이루어진 VPN에서의 실태점검 리스트를 (그림 2)에서와 같이 제시한다.

순서	항목	평가
1	외부에서 내부시스템 접근시 VPN을 이용하고 있는가?	
2	도입된 VPN장비는 보안성 검토를 득한 제품인가?	
3	VPN에 접근시 아이디/패스워드 이외에 다른 인증방식을 추가로 사용하고 있는가?	
4	VPN 접근 계정을 1인 1계정으로 사용하고 있는가?	
5	VPN 접근 계정의 패스워드를 6개월 마다 변경하고 있는가?	
6	인사정보시스템 및 AD 서버와 연동되어 있는가?	
7	VPN 사용시 사용신청 프로세스를 거쳐 진행하는가?	
8	VPN 접속 로그를 관리하고 있는가?	

(그림 2) VPN 실태점검 체크리스트



(그림 3) VPN에서의 이상행동 탐지를 위한 시나리오

3.2 VPN 접속시 이상행동 탐지를 위한 시나리오 도출

VPN을 통해 원격지에서 업무시스템에 접근이 용이한 반면, 중요정보들에 대한 유출 위험성이 존재하게 된다. 이를 대응하기 위해 VPN의 접속로그들을 분석하여, 구성원의 이상행동 탐지를 해야 한다. 따라서 VPN에서 발생하는 로그 테이블 및 필드정보에 대해 “식별정보”, “정보유출 시나리오 정보”, “분석정보” 필드로 구분하여 로그정보를 분석 후 “정보유출 시나리오 정보” 필드에 따라 이상행동 탐지를 위한 시나리오를 (그림 3)과 같이 도출하였다.

4. 결론

본 논문에서는 원격지에서 내부 업무시스템에 접속하기 위해 사용 중인 VPN의 실태점검 체크 리스트를 제시하였고, VPN에서 발생하는 접속 로그정보를 분석하여 정보유출의 이상행동의 탐지를 위한 시나리오를 도출하였다.

제시한 실태점검 체크리스트를 통해 각 업무 담당자는 VPN 운영의 현 상황을 파악할 수 있으며, 어떻게 운영하고 관리해야하는지 가이드라인이 될 수 있다. 또한 VPN에서의 이상행동 탐지를 위한 시나리오를 이용하여 정보유출방지 통합 모니터링에 적용할 수 있다.

참고문헌

[1] 박장수, 박정현, 강용석, 이임영, “사용자 행위 Modeling을 이용한 내부정보유출 방지 시나리오 설계방안에 관한 연구,” 한국정보처리학회 추계학술발표대회 논문집, 제 20권, 제 1호, 2013

[2] 김송영, 김요셉, 임종인, 이경호, “빅데이터를 이용한 보안정책 개선에 관한 연구,” 한국정보보호학 논문지, 제 23권, 제 5호, 2013

[3] 김두상, 김성락, “어플리케이션 로그를 활용한 정보유출 징하 모니터링 연구”, 한국정보기술학회 학회지 제 11권, 제 8호, 2013

[4] 박장수, 이임영, “정보유출방지 보안솔루션 로그 분석 방안에 관한 연구 - 정보유출 단일 시나리오를 중심으로”, 한국정보보호학회 충청지부 학술발표대회 논문집, 2014